

## (FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	Benefits, healthcare & research	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Benefits, healthcare & research	Written	Written
Service Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Medical Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Criminal Record Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Guardian Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Education Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Benefit Information	Paper & Electronic	Benefits, healthcare & research	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Criminal Record Information	No			
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written
Other (Explain)				
Other (Explain)				
Other (Explain)				

### **Welcome to the PIA for FY 2010!**

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

### **Directions:**

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: <http://vawww.privacy.va.gov/PIA.asp>

### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

**Definition of PII (Personally Identifiable Information)**

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

**Macros Must Be Enabled on This Form**

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

## (FY 2010) PIA: System Identification

---

Program or System Name:	Region 4>VHA>VISN 03> VANJHCS >LAN
OMB Unique System / Application / Program Identifier	(AKA: UPID #): 029-00-02-00-0101120-00

The LAN system is the hardware infrastructure on which the VHA health care facilities operate their software applications and support for E-Government initiatives to include Picture Archiving and Communication Systems (PACS). The PACS applications in VISN 3 LAN systems include radiology, cardiology, optometry and dental. Note that PACS is a generic term for anything that archives images. Radiology, Cardiology, Optometry, and Dental utilize PACS for their departments. It includes the computer equipment associated with clinical operations and the employees (approximately 3000 FTE) necessary to operate the system. LAN system supported IT

Description of System / Application / Program: services across the VA

VA New Jersey Health Care System			
Facility Name:			
Title:	Name:	Phone:	Email:
		(973) 676-	
Privacy Officer:	Helen Hollins	1000 ext 3475	<a href="mailto:Hellen.Hollins@va.gov">Hellen.Hollins@va.gov</a>

Information Security Officer:	Kathy DeVierno	908 604-5299	<a href="mailto:kathleen.devierno@va.gov">kathleen.devierno@va.gov</a>
Chief Information Officer:	Scott Soldan	(908) 647-0180 ext. 4615	<a href="mailto:Scott.Soldan@va.gov">Scott.Soldan@va.gov</a>
Person Completing Document:	Kathy DeVierno	908 604-5299	<a href="mailto:kathleen.devierno@va.gov">kathleen.devierno@va.gov</a>
Other Titles:			
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	Full PIA 8/1/2008 & PIA Validation 07/2009		
Date Approval To Operate Expires:	08/2011		

---

What specific legal authorities authorize this program or system:

Privacy Act, 5 U.S.C.552A

What is the expected number of individuals that will have their PII stored in this system:

50,000 to 100,000

Identify what stage the System / Application / Program is at:

Operation/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

Operational since 1995 – 13 years

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Has a PIA been completed within the last three years?

Yes

---

Date of Report (MM/YYYY):

08/2008

---

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.**

- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

**Regio**

## (FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

79VA19

2. Name of the System of Records:

VistA-VA

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

***(Please Select Yes/No)***

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

### (FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA New Jersey Health Care System	Yes	Veteran Information	Both PII & PHI	day to day operations
Other Veteran Organization	VBA	No	Veteran Information	Both PII & PHI	VA internally shares clinical and Administrative data with the VBA for the purpose of ensuring benefits are received
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

### (FY 2010) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system:

Per responses in Tab 4, does the system gather information from an individual? No

If information is gathered from an individual, is the information provided:

☐ Through a Written Request

☐ Submitted in Person

☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down? Yes

### (FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? No

- ☐ Drug/Alcohol Counseling      ☐ Mental Health      ☐ HIV  
☐ Research    ☐ Sickle Cell    ☐ Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access  
to this data.

Answer:

## (FY 2010) PIA: Program Level Questions

---

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

Yes  
Veteran  
personal  
informati  
on and  
informati  
on vital to  
the  
operation  
of the  
medical  
center

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Users just  
enter the  
data they  
need

Answer:

How is data checked for completeness?

Answer:

User are  
responsibl  
e for  
updating  
the  
informati  
on in their  
network  
folders

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

User are  
responsibl  
e for  
updating  
the  
informati  
on in their  
network  
folders

---

How is new data verified for relevance, authenticity and accuracy?

Answer:

Responsib  
ilty of the  
user

---

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

---

## (FY 2010) PIA: Retention & Disposal

---

What is the data retention period?

Varies  
according  
to the  
record  
control  
schedule

Answer:

Explain why the information is needed for the indicated retention period?

Health  
care and  
business  
requirem  
ents

Answer:

What are the procedures for eliminating data at the end of the retention period?

Answer:

Electronic  
Final  
Version of  
Patient  
Medical  
Record is  
destroyed  
/deleted  
75 years  
after the  
last  
episode of  
patient  
care as  
instructed  
in VA  
Records  
Control  
Schedule  
10-1,  
Item  
XLIII, 2.b.  
(Page  
190). At  
the  
present  
time,  
VistA  
Imaging  
retains all  
images

---

Where are these procedures documented?

Answer:

national  
policies,  
RCS-10-1,  
current  
VA policy  
and NIST  
guidelines

---

How are data retention procedures enforced?

Answer:

Records  
Control  
Schedule  
10-1  
(page 8):  
Records  
Managem  
ent  
Responsib  
ilities The  
Health  
Informatio  
n  
Resources  
Service  
(HIRS) is  
responsibl  
e for  
developin  
g policies  
and  
procedure  
s for  
effective  
and  
efficient  
records  
managem  
ent  
throughou

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

### (FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

## (FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer:

Certification and Accreditation of system is conducted every 3 years and the system undergoes an annual self assessment as required by FISMA. Certification and Accreditation is ongoing in conjunction with IT and Information

Explain what security risks were identified in the security assessment? (Check all that apply)

- ☒ Air Conditioning Failure
- ☐ Chemical/Biological Contamination
- ☐ Blackmail
- ☐ Bomb Threats
- ☐ Cold/Frost/Snow
- ☒ Communications Loss
- ☐ Computer Intrusion
- ☐ Data Destruction
- ☐ Data Disclosure
- ☐ Data Integrity Loss
- ☐ Denial of Service Attacks
- ☐ Earthquakes
- ☐ Eavesdropping/Interception
- ☒ Fire (False Alarm, Major, and Minor)
- ☒ Flooding/Water Damage
- ☒ Hardware Failure
- ☒ Malicious Code
- ☐ Computer Misuse
- ☒ Power Loss
- ☐ Sabotage/Terrorism
- ☐ Storms/Hurricanes
- ☐ Substance Abuse
- ☐ Theft of Assets
- ☐ Theft of Data
- ☐ Vandalism/Rioting
- ☐ Errors (Configuration and Data Entry)
- ☐ Burglary/Break In/Robbery
- ☐ Identity Theft
- ☐ Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. (Check all that apply)

- ☒ Risk Management
- ☒ Access Control
- ☒ Awareness and Training
- ☒ Contingency Planning
- ☒ Physical and Environmental Protection
- ☒ Personnel Security
- ☒ Certification and Accreditation Security Assessments
- ☒ Audit and Accountability
- ☒ Configuration Management
- ☒ Identification and Authentication
- ☒ Incident Response
- ☒ Media Protection

loss of availability could be expected  
adverse effect on operations, assets  
or individuals.

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer:

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

Controls to mitigate the misuse

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?

(Choose One)

☒

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

☐

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?

(Choose One)

☒

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

☐

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?

(Choose One)

☒

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

☐

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

## (FY 2010) PIA: Additional Comments

---

Add any additional comments on this tab for any question in the form you want to comment on.  
Please indicate the question you are responding to and then add your comments.

---

(FY 2010) PIA: VBA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Record Interchange (CAPRI)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Control of Veterans Records (COVERS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Synquest
Veterans Exam Request Info System (VERIS)	Fiduciary Beneficiary System (FBS)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Hearing Officer Letters and Reports System (HOLAR)	ASSISTS
	Inforce	
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	Name		Description		Comments
	<input type="checkbox"/> Is PII collected by this min or application?				
	<input type="checkbox"/> Does this minor application store PII?				
	If yes, where?				
	Who has access to this data?				

Minor app #2	Name		Description		Comments
	<input type="checkbox"/> Is PII collected by this min or application?				
	<input type="checkbox"/> Does this minor application store PII?				
	If yes, where?				
	Who has access to this data?				

Minor app #3	Name		Description		Comments
	<input type="checkbox"/> Is PII collected by this min or application?				
	<input type="checkbox"/> Does this minor application store PII?				
	If yes, where?				
	Who has access to this data?				

---

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Asisstant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitelment Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	SUPPORT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION	KERNEL
AUTOMATED LAB INSTRUMENTS	SYSTEM	KIDS
AUTOMATED MED INFO EXCHANGE	EQUIPMENT/TURN-IN	LAB SERVICE
BAR CODE MED ADMIN	REQUEST	LETTERMAN
BED CONTROL	EVENT CAPTURE	LEXICON UTILITY
BENEFICIARY TRAVEL	EVENT DRIVEN REPORTING	LIBRARY
CAPACITY MANAGEMENT - RUM	EXTENSIBLE EDITOR	LIST MANAGER
CAPRI	EXTERNAL PEER REVIEW	MAILMAN
CAPACITY MANAGEMENT TOOLS	FEE BASIS	MASTER PATIENT INDEX
CARE MANAGEMENT	FUNCTIONAL	VISTA
CLINICAL CASE REGISTRIES	INDEPENDENCE	MCCR NATIONAL
CLINICAL INFO RESOURCE NETWORK	GEN. MED. REC. - GENERATOR	DATABASE
CLINICAL MONITORING SYSTEM	GEN. MED. REC. - I/O	MEDICINE
CLINICAL PROCEDURES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL REMINDERS	GENERIC CODE SHEET	MICOM
CMOP	GRECC	MINIMAL PATIENT
CONSULT/REQUEST TRACKING	HEALTH DATA &	DATASET
CONTROLLED SUBSTANCES	INFORMATICS	MYHEALTHVET
CPT/HCPCS CODES	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)
CREDENTIALS TRACKING	HEALTH SUMMARY	A4EL
DENTAL	HINQ	NATIONAL DRUG FILE
DIETETICS	HOSPITAL BASED HOME	NATIONAL LABORATORY
DISCHARGE SUMMARY	CARE	TEST
DRG GROUPER	ICR - IMMUNOLOGY CASE	NDBI
	REGISTRY	NETWORK HEALTH
	IFCAP	EXCHANGE
	IMAGING	NOIS
	INCIDENT REPORTING	NURSING SERVICE
	INCOME VERIFICATION MATCH	OCCURRENCE SCREEN
	INCOMPLETE RECORDS	ONCOLOGY
	TRACKING	ORDER ENTRY/RESULTS
		REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description		Comments
Minor app #1			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #2			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #3			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

---

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING
MEDICINE	
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #2	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #3	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

## (FY 2010) PIA: Final Signatures

Facility Name: VA New Jersey Health Care System

Title:	Name:	Phone:	Email:
Privacy Officer:	Helen Hollins	(973) 676-1000 ext 3475	Hellen.Hollins@va.gov
Digital Signature Block			
Information Security Officer:	Kathy DeVierno	908 604-5299	kathleen.devierno@va.gov
Digital Signature Block			
Chief Information Officer:	Scott Soldan	(908) 647-0180 ext. 4615	Scott.Soldan@va.gov
Digital Signature Block			
Person Completing Document:	Kathy DeVierno	908 604-5299	kathleen.devierno@va.gov
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report:

8/7/2008

OMB Unique Project Identifier

029-00-02-00-0101120-00

Project Name

Region 4>VHA>VISN 03> VANJHCS  
>LAN